ISBN: 978-93-6773-974-7

EFFECTIVENESS AND CHALLENGES OF AI-POWERED INTRUSION DETECTION SYSTEMS

ROHIT KAPOOR
ASSISTANT PROFESSOR
LUCKNOW PUBLIC COLLEGE OF PROFESSIONAL STUDIES

KEYWORDS

ARTIFICIAL INTELLIGENCE, INTRUSION DETECTION SYSTEMS, DEEP LEARNING, CYBERSECURITY, NETWORK SECURITY, ANOMALY DETECTION.

ABSTRACT

As technology advances rapidly and the internet spreads, computer systems are increasingly vulnerable to diverse forms of cyber threats. To combat sophisticated attacks, traditional intrusion detection system (IDS) are not sufficient enough; therefore, the implantation of artificial intelligence (AI) in cybersecurity framework is highly needed. In this paper we explore how AI based intrusion detection works and highlighting its potential advantages to help us catch threats. We also discuss the challenges in their implementation, such as data privacy issues, algorithmic bias and the requirement to regularly update algorithms to counteract new threats.

In this paper, we explore the utilization of Artificial Intelligence (AI) and deep learning methods in Intrusion Detection Systems (IDS) as a proactive approach to safeguarding networks and ensuring no malicious intrusions occur, especially given that cyber threats continue to grow in complexity and numbers. Conventional security measures proved to be insufficient against intricate attacks, requiring the design of advanced IDS, adept at detecting threats in real-time. This study demonstrates the application of deep learning to the evolution of cyber threat environment. In addition, the paper discusses important challenges of AI-powered IDS, such as the quality of data, computational resource requirements, and the lack of explainability of these AI models that inhibits the creation of trust between users and AI models. This

research seeks to contribute to current discussions on improving cybersecurity by deriving new AI-relevant applications in intruder detection through an in-depth analysis of these elements.

1. INTRODUCTION

For organizations to mitigate sophisticated cyber-attacks, they are required to bolster their security strategies. Important to identifying and responding to malicious activities within networks are Intrusion Detection Systems (IDS). AI technologies, including machine learning and deep learning, have been implemented in the form of artificial intelligence-supported IDS that can improve detection rates with fewer false positives. However, even though these systems provide considerable benefits, they also entail challenges. We wish to explore AI-based IDS focus on the pros and cons, with some recommendations for enhancing these aspects in the cybersecurity arena over the long term. As cyber threats continue to expand, filtering out conventional security methods is less and less effective in protecting critical infrastructure and sensitive information. IDS have become critical components in cybersecurity strategies, aiding in the detection of malicious actions or violations of policy.

However, IDS is rule and signature based and hence, are oblivious to novel and advanced attack types. One of or approach toward adapting this vacuum is the enlistment of computer science and principles of machines in the domain of intrusion detection systems (IDS), where machines are helped by ML and polarities them identifying to respond to their incoming threats in real-time. AI is used to develop the strategy of an IDS that analyzes the data using sophisticated algorithms to detect unusual patterns and detect intrusion. Not only they are trained on models that are capable of detecting attacks during their existence, you use them to increase performance based upon past events, you can even adapt the solution for attacks that become exposed. Ai algorithms are capable of detecting sudden changes in user activity and behavioural deviations on interconnected networks that would alert to an attack, allowing organizations to take preventive measures before damage is done.

Hyper accurate threat detections are just a small piece of the secret that has enabled AI to scale in this space, as is the jarring decrease in false positives. Traditional security intrusion detection systems can generate alarm fatigue for security people, who are inundated with false positives. On the contrary, AI

powered systems do context aware data analysis and eliminate the false positives and arm the security personnel with actionable insights. What supports the scalability of AI technologies in different environments is the scale properties of such things; it can competently cover a high-bandwidth of information regardless of the size of the environment, from small businesses to enormities. The AI powered IDS has many advantages but also have Challenges. These may have limitations associated with the quality and availability of relevant data. Machine learning models use enormous quantities of data, which begs the question, how reliable and trustworthy is the information they are utilising as a training dataset? Other than that cyber threats are consistently changing so it needs to evolve the AI algorithms consistently and continuously." Interpreting AI decisions only complicates the issue further regarding trust and accountability in security operations. In this paper, we present the latest studies from traditional IDSs up to AI-based intrusion detection systems with a focus on performance and constraints. It will also evaluate the progress toward this idea, as well as the ways that success for such systems should be measured, and what all of this means for the future of cyber security R&D

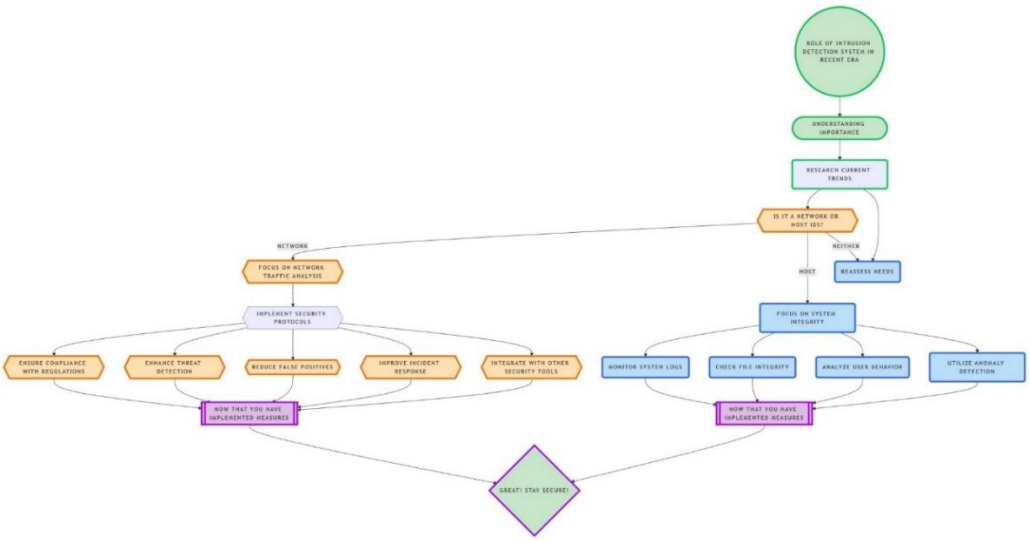

FIG 1: OPERATION OF DIFFERENT INTRUSION DETECTION SYSTEM

2. LITERATURE REVIEW ON AI-POWERED INTRUSION DETECTION SYSTEMS

With the growing complexity of cyber threats and the limitations of conventional detection techniques, the use of Artificial Intelligence (AI) in Intrusion Detection Systems (IDS) has attracted a great deal of interest in recent years. This literature

survey presents the state of the art of artificial intelligence-based intrusion detection system in terms of detection, methodologies, and issues faced.

2.1 EFFECTIVENESS OF AI IN INTRUSION DETECTION

Over traditional systems, this leads to significant improvement in the detection accuracy and flexibility of the intrusion detection system (IDS). The use of artificial intelligence (AI) in IDS enhances the ability to detect and classify network traffic, as well as detect anomalous behavior, Markevych and Dawson (2023) that AI systems are trained on data from the past; therefore, they are able to identify patterns that are indicative of malicious behavior, enabling even the detection of unknown threats. This flexibility is necessary to detect APTs (advanced persistent threats), and zero-day exploits, which are typically built to evade all signature-based detection methods.

In addition, Xu et al. 2023) pointed out the plethora of studies on the utilization of machine learning (ML) and deep learning (DL) techniques for intrusion detection. Based on their evaluation of 393 studies, they've identified prominent algorithms in this domain, with a trend towards CNNs, SVMs, and decision trees. The results of our research reveal that the application of these AI methodologies considerably improves the security and scalability of the IDS, empowering the IDS to operate efficiently even with high volumes of data.

2.2 METHODOLOGIES EMPLOYED

AI-powered IDS utilizes a wide range of techniques which revolve around different kinds of machine learning and deep learning approaches. In this encompassing review, Sowmya and Anita (2023) divided the existing literature into three categories of techniques: machine learning, deep learning, and ensemble learning. As shown in the results of the study, not only have researchers developed significant methods to improve detection performance, there has also been a substantial deficiency in focused action against the precise attack type2. Not only that but research shows successful deployments across a range of industries. For example– research of Kanimozhi and Jacob, presents an AI-based Neural Network-based system helps in Identifying botnet attacks in the banking domain. Their study findings demonstrated that. This system trained on the CSE-CIC-IDS2018 dataset, proving that AI-driven intrusion detection systems could strengthen security in high-risk contexts.

2.3 CHALLENGES FACED BY AI-POWERED IDS

While the benefits of AI-powered intrusion detection systems are vast, a number of barriers hinder their widespread adoption. Data quality is a significant concern, as Markevych and Dawson (2023) illustrate, biases in training data can lead to inaccurate predictions and lower effectiveness 1.

Another aspect that brings enterprises with limited resources into trouble regarding computational complexity is that working with advanced artificial intelligence algorithms can require a really high level of processing power. Another major barrier to overcome is the challenge of explaining AI models. It has been stated in the study conducted by Sowmya and Anita (2023) that the non-transparency in the decision-making process of the artificial intelligence systems is likely to diminish trust on the part of the users and complicate the efforts of incident response

Addressing these challenges is crucial if we want to harness the potential of artificial intelligence technologies for intrusion detection.

Intrusion Detection Systems: Keeping Up with Cyber Security When AI Meets Cyber Security These rebinds, both provide enhanced detection abilities and the ability to respond to new threats. However, to take full advantage of these technologies it is essential to address challenges related to the quality of the data, the computing requirements and the explainability of the models. As AI techniques within IDS need to be improved and must be able to meet the dynamic nature of evolving cyber threats, constant research is highly important in this regard.

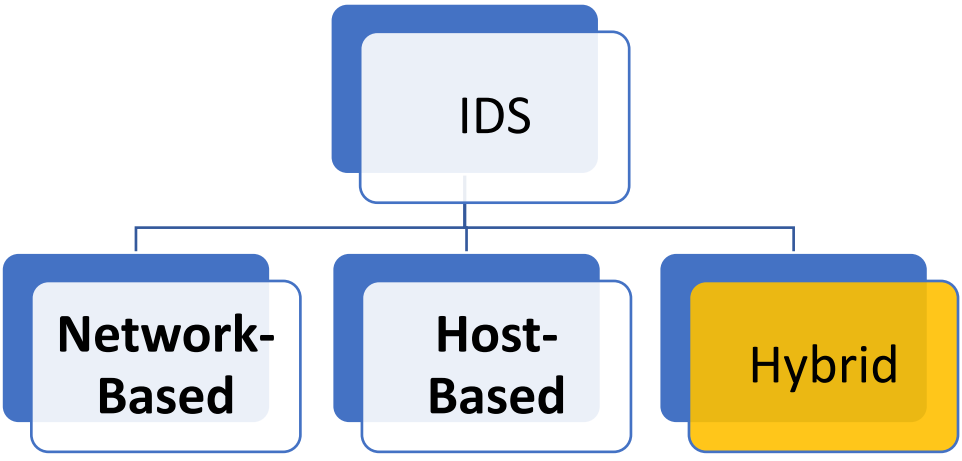

FIG 2: TYPES OF INTRUSION DETECTION SYSTEM

2.4 Traditional IDS vs. AI-Powered IDS

Traditional Intrusion Detection Systems (IDSs) are typically rule or signature-based and are thus vulnerable to zero-day attacks. In contrast, traditional IDSs are too dependent on rule sets and signatures, making them inadequate against sophisticated attack techniques.

Aspect	AI-Powered Intrusion Detection Systems	Manual Intrusion Detection Systems
Detection Methodology	Detects abnormalities and analyses data patterns in real time using machine learning and deep learning.	Relies on predefined rules and signatures to identify known threats.
Adaptability	Adapts to changing threats and improves detection accuracy by learning from fresh data.	Limited adaptability; requires manual updates to rules and signatures to recognize new threats.
Response Mechanism	Can automatically ban IP addresses or isolate impacted systems to respond to attacks.	Typically requires manual intervention for response actions, which can delay reaction times.
False Positive Rate	Advanced anomaly detection distinguishes benign from harmful activity, reducing false positives.	Higher false positive rate due to reliance on static rules, which may not account for nuanced behaviours.
Data Analysis	Fastly processes vast amounts of data to find complicated relationships and patterns that may reveal intrusions.	Limited data analysis capabilities; often relies on human analysts to interpret logs and alerts, which can be time-consuming.
Scalability	Scalable to handle more data and bigger networks without performance compromise.	Less scalable; may require additional resources and personnel as the network grows, leading to increased operational costs.
Implementation Complexity	Integration with current systems, training models, and	Simpler implementation; often involves setting up rule-

	continuous learning make implementation more difficult.	based systems with less technical complexity.
Cost Efficiency	Initial setup is expensive, but less manual labour and quicker threat response save money over time.	Lower initial costs, but ongoing expenses related to manual monitoring and potential incident response delays can accumulate over time.
Use Cases	Effective in highly variable traffic patterns or sophisticated attack settings	Suitable for smaller networks or environments where threats are well understood and predictable (e.g., small businesses).
Detection Methodology	Utilizes machine learning and deep learning algorithms to analyze data patterns and detect anomalies in real-time.	Relies on predefined rules and signatures to identify known threats.
Adaptability	Makes use of methods for machine learning and deep learning to examine data trends and spot irregularities as they happen.	Limited adaptability; requires manual updates to rules and signatures to recognize new threats.
Response Mechanism	Adapts to changing threats and improves detection accuracy by learning from fresh data.	Typically requires manual intervention for response actions, which can delay reaction times.
False Positive Rate	Generally has a lower false positive rate due to advanced anomaly detection capabilities that differentiate between benign and malicious activities.	Higher false positive rate due to reliance on static rules, which may not account for nuanced behaviours.

Data Analysis	Capable of processing large volumes of data quickly, identifying complex patterns and correlations that may indicate intrusions.	Limited data analysis capabilities; often relies on human analysts to interpret logs and alerts, which can be time-consuming.
Scalability	Highly scalable; can handle increasing amounts of data and adapt to larger networks without significant performance degradation.	Less scalable; may require additional resources and personnel as the network grows, leading to increased operational costs.
Implementation Complexity	Works well in places where traffic patterns are very unpredictable or where complex assaults are anticipated	Simpler implementation; often involves setting up rule-based systems with less technical complexity.

TABLE 1.1 TRADITIONAL IDS VS. AI-POWERED IDS

3. EFFECTIVENESS OF AI-POWERED INTRUSION DETECTION SYSTEMS

3.1 ENHANCED DETECTION CAPABILITIES

AI-Driven IDS can greatly enhance detection rates by:

- **Pattern Recognition:** AI algorithms can detect intricate patterns in the data that might suggest a potential attack, which conventional systems may miss.
- **Anomaly Detection:** Using machine learning algorithms, systems can analyse large volumes of network data to create baselines of normal behaviour and identify anomalies that may indicate intrusions.

3.2 REDUCED FALSE POSITIVES

The ability to reduce false positives is one of the advantages of the AI-powered IDS. It serves as a common review point for security professionals or those providing additional machine learning detection capabilities with and instead to improve overall system detection efficiency.

3.3 ADAPTABILITY AND LEARNING

Ability to learn is essential for detecting and responding to any advances regarding cyber threats. The challenge for IDS lies in adapting to new behavior patterns and

focusing on detecting unknown threats as they evolve with more advanced attack vectors. Based on some of the recent research, this section discusses ways of improving adaptability and learning in IDS.

3.4 ADAPTIVE LEARNING TECHNIQUES

Ensemble Learning: Several state-of-the-art IDS systems employ ensemble learning techniques where multiple machine learning models are combined to enhance detection performance. Systems that mix decision trees, Random Forests, and other classifiers are able to learn adaptively with respect to a large set of attacks. In this way IDS will take advantage of its algorithms strengths reducing its weaknesses improving the overall performance

3.5 HANDLING CONCEPT DRIFT

Dealing with Concept Drift: Concept Drift refers to changes in the statistical properties of an observed process over time, and is yet another major challenge for IDS. This leads to a drop in performance, as the system is less capable of identifying new attack types due to concept drift. It means that adaptive IDS should develop very sophisticated algorithms that can detect specific behaviours of malicious attacks and then update their model depending on changes in the data distribution automatically.

3.6 HYBRID APPROACHES

Merging multiple learning techniques with supervised and unsupervised learning can improve the adaptability of an IDS to new threats. While supervised learning can be applied to classify known types of attacks, unsupervised learning can also be employed to discover anomalies in data, thereby aiding the detection of zero-day attacks or novel patterns of intrusion. This combined methodology enables a broader detection strategy that adapts to and evolves with developing threat environments

3.7 TRAFFIC FILTERING

By using traffic filters to eliminate non-malicious packets, it can relieve the computational load from the IDS focus on potentially harmful traffic. This helps reduce response times and reduce false positives as adaptive IDS can filter out the relevant traffic for analysis.

3.8 EXPERIMENTAL VALIDATION

The effectiveness of adaptive learning techniques for intrusion detection systems will need to be evaluated empirically. Based on research conducted using datasets such as CIC-IDS2017, we can conclude that adaptive systems performed better in terms of performance metrics than traditional models, showing that they could be implemented for online threat detections and exhibited lower rates of false positives at the same time. Intrusion Detection Systems (IDS) must continuously adapt and learn in order to mitigate new malicious threats to cyber security. Ensemble learning, incremental learning, concept drift handling, online learning, and traffic filtering can improve the precision and responsiveness of such systems. Until threat surfaces are effectively addressed by a much more comprehensive approach, continued investment to keep R&D will be essential to develop an effective cyber-shield, as threat surfaces are evolving rapidly in terms of their complexity as well.

4. CHALLENGES OF AI-POWERED INTRUSION DETECTION SYSTEM

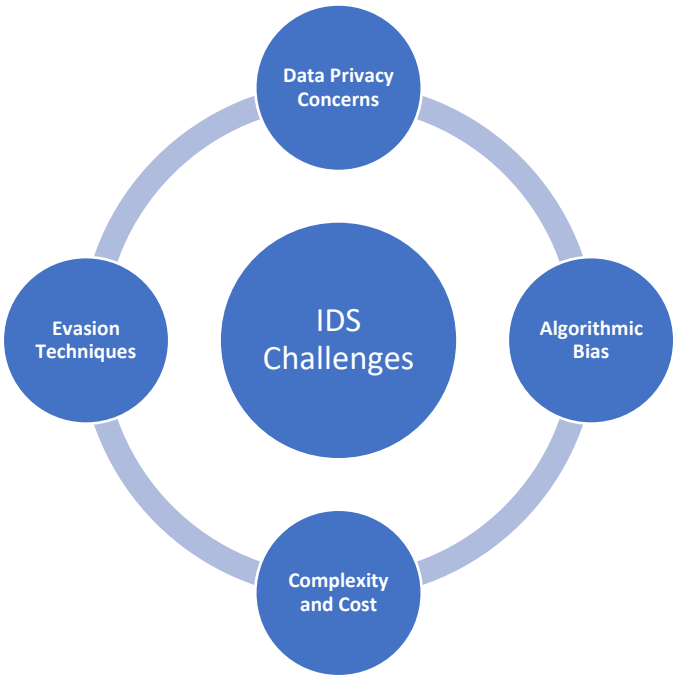

FIG 3: AI POWERED IDS CHALLENGES

4.1 Data Privacy Concerns

Even though these AI-based IDS implementations might need to extract and analyze lots of sensitive information, on an ongoing basis. Here organizations have to balance security constraints against user privacy constraints mandated by laws such as GDPR.

FIG 4: DATA PRIVACY CONCERNS

4.2 ALGORITHMIC BIAS

AI algorithms are fed training data, and if the data is biased, the AI generated data will also be biased. All algorithms are biased, but if the training data is biased then it can make for skewed results and inequality of detection rates across different demographic groups.

4.3 COMPLEXITY AND COST

It is also costly and complex to develop and deploy an AI- based IDS. This means ubers will need to deploy capital on technology and people and maintenance of these platforms.

4.3.1 COST FACTORS IN IDS

- **Development Costs:** Implementing an IDS requires hardware and the installation, configuration, and setup of software. Costs in these categories can range from highly variable based on the capabilities of the system, and some more exacting organizational needs [1] [3].
- **Operational Expenses:** Ongoing costs over a system's lifetime, such as ongoing maintenance, updates, and personnel time to monitor the system are also included in some rough list of costs over a system's life — and the lifetime operational costs are often far larger than the previous design and setup costs, particularly if human supervision or additional systems are necessary.
- **Damage Costs:** Cost of damage when a successful intrusion occurs through IDS Fail or false-positive. Organizations must assess probable loss due to the data breach or service disruption when gauging an IDS's effectiveness.
- **Response Costs:** Expenses incurred due to response to detected threats, these may be any expenses incurred for incident response teams, forensics and remediation in the effort to mitigate the effect of the incident on the business. High false positive lead levels can drastically inflate such costs in such cases.

4.3.2 COMPLEXITY OF IDS

- **System Complexity:** An IDS can suffer from its own complexity; a simpler system a lot of the time means lower operations barriers further down the road. Some Alert Patterns are confounding to Understand Multi–actions alerts are a feature of your management and in correct alerts interpreting you, red alerts loop increase, and ratio more real risk alerts are being discarded.
- **Complexity of the System:** Implementing IDS as part of a comprehensive security architecture introduces complexity that may demand significant preparation and resource investment. From management and alert interpretation perspective, this can lead to longer reaction time and chance of missed alerting true threat as more and more alerts would require to be responded.
- **Integration Issues:** A further challenge could be integrating IDS into an organization which can take time and resources to plan out their use in relation to the existing security infrastructure integration is another challenge. This can cause compatibility issues for those not using the same system, and may lead to operational inefficiencies.
- **Scalability Challenges:** With the growth of an organization, its security requirements change. An IDS needs to scale without a commensurate increase in operational costs or performance degradation. This level of scalability is often difficult for traditional systems to achieve

FIG 5. COST FACTOR

4.4 EVASION TECHNIQUES

More sophisticated evasion techniques that challenge the limitations of AI-enabled IDS are leveraged by the cybercriminals. The inputs to these systems can be manipulated so that they provide wrong predictions, referred to as adversarial attacks, highlighting the necessity for continuous evolution of detection techniques.

5. FUTURE DIRECTIONS

To enhance the effectiveness of AI-powered IDS, future research should focus on:

- **Hybrid Approaches**: Combining AI with traditional methods to leverage the strengths of both systems.
- **Explainable AI**: Developing algorithms that provide insights into their decision-making processes, thereby improving transparency and trust.
- **Robustness Against Evasion**: Creating more resilient systems capable of withstanding adversarial attacks through continuous learning and adaptation.

The future of Intrusion Detection Systems (IDS) is shaped by emerging technologies, evolving cyber threats, and the need for more integrated security solutions. Below are key trends and directions identified in the search results:

5.1 INTEGRATION OF AI AND MACHINE LEARNING

AI and machine learning will play a crucial role in enhancing the capabilities of IDS. These technologies can analyse vast amounts of data to detect anomalies more accurately than traditional methods, allowing for real-time threat detection and response . The next generation of IDS will probably move towards being more adaptable, adjusting their responses by observing the behaviour of users and the network.

5.2 CLOUD-BASED SOLUTIONS

Growth of Cloud-Based IDS Solutions Due To Adoption of Cloud Technology These systems also provide scalability and flexibility while minimizing infrastructure burdens for organisations. And as more businesses are moving their operations to alignment with cloud environments, the need for a strong cloud-native IDS system will take off.

5.3 INTEGRATION WITH OTHER SECURITY PRODUCTS

So, IDS is definitely on the cards and therefore indicates a clear move towards integrating it together with other security solutions in one cohesive security posture. For instance, it includes interoperable between firewalls, endpoint protection, and threat intelligence platforms. Those integrations would further improve overall security effectiveness by providing a holistic view of threats across disparate environments.

5.4 FOCUS ON EMERGING THREATS

According to the increasing advanced cyber threats like zero-day attacks, advanced persistent threats (APTs), ransomware, and DDoS attacks, IDS have to be upgraded to meet the changes as per the market. The next generation systems will have to incorporate complex detection methods to detect these sophisticated threats that can evade the traditional defences.

5.5 OPEN PLATFORMS AND THIRD-PARTY INTEGRATIONS

They are looking for open platforms enabling interoperability with third-party solutions. This approach highlights the need for interoperability between security solutions, allowing organizations to tailor their security process to their requirements. Flexibility will be a core element to adapt to different security needs.

5.6 ENHANCED SCALABILITY AND PERFORMANCE

The future IDS will be based on ever-increasing data coming from IoT devices and 5G networks. Such systems should be able to be scaled up smoothly, keeping performance levels up. Your extensive supply of data will always be needed for real-time threat detection.

5.7 ADOPTION OF EDGE COMPUTING

Therefore, modern IDS can be seen that the tools and to choose from for the industry, IPI technology is expected to move towards the edge computing era. This will enable faster threat detection and response, especially relevant to IoT environments.

5.8 ETHICAL CONSIDERATIONS AND DATA PRIVACY

With the deeper integration of AI within IDS, ethical issues concerning data privacy and algorithmic bias will become more prominent. Compliance with regulations remains a challenge for organizations, however, organizations must leverage AI technologies for intrusion detection while also ensuring compliance with regulations in place.

ML, DL have significant benefits over the status quo solutions such as false alarms in threat detection, scalability, interpretability, and false positives of these methods respectively. The future of Intrusion Detection Systems will be shaped by exciting developments in AI/ML techniques, cloud platform integration capabilities and above all a shift of focus from existing threats to emerging threats. In the era of evolving cyber threats, organizations should seek the innovative IDS solutions that do not merely stop at traditional detection capabilities but also providing a strong security framework tailored to their needs.

6. MEASURES FOR IMPROVEMENT

- **Improving Data Quality And Collection:** The machine learning model is trained with broad and extensive datasets to improve the anomaly detection capability of the model. Some random and attack traffic patterns are used so that it can learn to differentiate between legitimate and malicious. Enhancing incoming data on the fly with context (such as adding user behaviour or history

data) may help the IDS to assess whether an alarm is legitimate or not, and reduce type I error as well as increase detection rates.

- **Advanced Algorithms and ML Anomaly detection techniques:** It involves the use of advanced ML techniques such as SVM, Decision Trees, and deep learning models that can enhance the detection abilities of Intrusion Detection Systems (IDS). This makes them capable of detecting complex data patterns that signature-based techniques miss.
- **Hybrid Approaches:** Best practices are to combine detection approaches, combining signature-based and anomaly-based detection approaches to improve accuracy, for example. Using a statistical analysis and machine learning approach as a hybrid classifier could lower false positives whilst maintaining a high detection rate.
- **Implementing alert correlation methods** more recently actually analyzes multiple warnings together rather than every single one in isolation. Alerts that are similar is combined in a single event report through algebraic evidence type to minimize false positives by means of identifying alert linkages, since the importance of each Alert widely varies. Alert Prioritization: Context can assist security teams in prioritizing threats by correlating alerts with the threat severity while filtering out unnecessary alerts that are of lower priority to the organization.
- **In order to assist the IDS's algorithms:** As they become more effective, you may wish to implement a feedback mechanism whereby security analysts review alarms and provide input. By continuously learning, the system can adjust to changing threats, while also minimizing false positives.
- **Automated Tuning:** By injecting several real-time performance measurements IDS parameters can be tuned to reduce false alerts without sacrificing sensitivity.
- **Enhance User Profiling User Behaviour Analytics (UBA):** Set baselines for how users typically interact. Knowing how people usually behave and, therefore, how they use their devices enables the IDS to detect potential intrusions and minimize false positives.
- **Regular Updates:** Now, the threats evolve need fresh signatures, threat intelligence feeds and algorithm enhancements to IDS. An updated system minimizes false positive and false negative.To evaluate the system under different scenarios, regular testing with real attack mechanisms is beneficial. Those practical insights can help to optimize detection algorithms and thresholds.

7. CONCLUSION

Overall, AI based approach in intrusion detection systems leads to enhancement in detection rates with fewer false alarm rates; thus, revolutionizing cybersecurity. However, we cannot turn a blind eye to the challenges as it is adopted. Moreover, counters of data privacy concerns, methods to deal algorithmic bias, complexity and evasion methods for successful adoption of these systems are also imminent. The threat landscape is ever-changing and, thus, more research and development will have to be conducted to ensure that the AI based IDS is more effective and is able to battle more and more advanced threats. Data quality, advanced algorithms, alert correlation, continuous learning, user profile, and regular updates all play a role in improving intrusion detection systems and minimizing false positives. These ways can help companies strengthen the security and effectiveness of IDS.

8. REFERENCES

- Amrutkar, S. (2022). “A Survey on Intrusion Detection Systems: Classical, Contemporary, and Future Directions. *Journal of Cybersecurity and Privacy”*.
- Bhatia, M., & Kaur, H. (2021). “Machine Learning Techniques for Intrusion Detection: A Review. *International Journal of Computer Applications”*.
- Kwon, D. H., & Kim, J. (2021). “A Study on AI-Based Intrusion Detection Systems: Current Status and Future Prospects. *Computers & Security”*.
- Zhang, Z., & Zheng, X. (2022). “The Challenges of AI in Cybersecurity: A Critical Review. *Journal of Information Security and Applications”*.
- "Securing Your Network: The Power of AI in Intrusion Detection Systems." HC Robo. 2024-09-20.
- "Machine Learning and Artificial Intelligence in Intrusion Detection." Koorsen.
- Shaik, D.A. "AI-Based Intrusion Detection Systems." Insights2TechInfo. 2024-09-18.
- Ripla, A. "AI-Powered Intrusion Detection."
- Sowmya, T., & Anita, E.A.M. (2023). "A comprehensive review of AI based intrusion detection system." *Measurement and Sensors*, 28, 100827. doi:10.1016/j.measen.2023.100827 .
- Markevych, M., & Dawson, M. (2023) “A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (AI)”. *Journal of Information Systems*, 29(3). Retrieved from https://intapi.sciendo.com/pdf/10.2478/kbo-2023-0072

- Sowmya, T., & Anita, E.A.M. (2023). “A comprehensive review of AI based intrusion detection system”. *Measurement: Sensors*, 2800827. doi:10.1016/j.measen.2023.100827.
- Xu et al. (2023). “Systematic literature review on intrusion detection systems: Utilization of ML, DL, optimization algorithms, and datasets from 2018 to 2023. *Measurement: Sensors*.https://ui.adsabs.harvard.edu/abs/2023MeasS..2800827S/abstract
- Kanimozhi, S., & Jacob, T.P. (2023).” An Artificial Neural Network-oriented system for identifying botnet attacks in banking services using CSE-CIC-IDS2018 dataset”.
- "Artificial Intelligence Based Intrusion Detection Techniques - A Review." ResearchGate publication on various AI techniques applied in network security contexts.
- "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection." Wiley Online Library publication discussing various AI methodologies in IDS applications.